418 Rec'd PCT/PTO 26 FEB 1999

FORM PTO-1390 (REV 1-98) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: EJK:6088

U.S. APPLICATION NO (If known, see 37 CFR 1.5): 09/242974

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/FR98/01343	25 June 1998	26 June 1997

TITLE OF INVENTION: UNPREDICTABLE MICROPROCESSOR OR MICROCOMPUTER

APPLICANT(S) FOR DO/EO/US: Michel UGON

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [x] This is a FIRST submission of items concerning a filing under 35 U.S.C. 371.
2. [ ] This is a SECOND or SUBSEQUENT submission of items concerning a filing under 35 U.S.C. 371.
3. [x] This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. [x] A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. [x] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [ ] is transmitted herewith (required only if not transmitted by the International Bureau).
   b. [xx] has been transmitted by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Office (RO/US).
6. [x] A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. [ ] Amendments to the claims of the International Aplication under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] have been transmitted by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [ ] have not been made and will not be made.
8. [ ] A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. [x] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. [ ] A translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. [x] An Information Disclosure Statement under 37 CFR 1.97 and 1.98. with references & International Search Report
12. [x] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included. to BULL CP8 & PTO Form 1595
13. [x] A FIRST preliminary amendment.
    [ ] A SECOND or SUBSEQUENT preliminary amendment.
14. [ ] A substitute specification.
15. [ ] A change of power of attorney and/or address letter.
16. [x] Other items or information: CYS PCT DEMANDE: PCT/RO/101; PCT/IB/301 & 308
    PROPOSED DRAWING CORRECTIONS

U.S. APPLICATION NO. (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
	PCT/FR98/01343	EJK:6088

17. ☒ The following fees are submitted:	CALCULATIONS PTO USE ONLY	
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO $970.00		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO $840.00		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO $760.00		
International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) $670.00		
International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) $96.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 970.00	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	$	
Total claims	31 - 20 =		x $18.00	$ 198.00	
Independent claims	1 - 3 =		x $78.00	$	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ $260.00	$	
TOTAL OF ABOVE CALCULATIONS =				$	
Reduction of 1/2 for filing by small entity, if applicable. A Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28). +				$	
SUBTOTAL =				$1,168.00	
Processing fee of $130.00 for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				$	
TOTAL NATIONAL FEE =				$1,168.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property +				$ 40.00	
TOTAL FEES ENCLOSED =				$1,208.00	
				Amount to be refunded:	$
				charged:	$

a. ☒ A check in the amount of $ 1,208.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 11-0610 . A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Edward J. Kondracki
KERKAM, STOWELL, KONDRACKI & CLARKE, P.C.
Two Skyline Place, Suite 600
5203 Leesburg Pike
Falls Church, VA. 22041

Edward J. Kondracki
SIGNATURE

EDWARD J. KONDRACKI
NAME

20,604
REGISTRATION NUMBER

Docket 6088
BULL 3630/BC

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (D.O./E.O./US)

Applicant:	Michel UGON
International Application No.:	PCT/FR98/01343
International Filing Date:	25 June 1998
U.S. Serial No.:	To be Assigned
U.S. Filing Date:	February 26, 1999
For:	"UNPREDICTABLE MICROPROCESSOR OR MICROCOMPUTER"

Falls Church, Virginia

PRELIMINARY AMENDMENT

Honorable Commissioner of Patents
and Trademarks
Washington, D.C. 20231

Sir:

Please amend the subject application, filed concurrently herewith, as indicated below:

IN THE SPECIFICATION:

After the title and before the first paragraph on page 1, insert the following heading centered:

--BACKGROUND OF THE INVENTION--;

After the title and before the first paragraph on page 1, insert the following heading at the left-hand margin:

--FIELD OF THE INVENTION--;

Page 1, after the first paragraph and before the second paragraph at line 2, insert the following heading at the left-hand margin:

--DESCRIPTION OF RELATED ART--;

Page 1, line 7, after "time", insert a comma --,--;

Page 1, line 11, delete "instructions" and substitute --instruction--;

Page 1, line 11, after "accurately", insert a comma --,--;

Page 1, line 13, after "processor", insert a comma --,--;

Page 3, lines 6 and 7, delete "the request for French Patent No. 9602903 of March 07, 1996 made" and substitute --application Serial No. 08/945,845 filed--;

Page 3, line 7, after "applicant", insert --on November 7, 1997 and--;

Page 3, lines 7 and 8, delete "improved integrated circuit, process for use of such integrated circuit" and substitute --Improved Integrated Circuit And Process For Using An Integrated Circuit",--;

Page 4, before the first full paragraph at line 1, insert the following heading at the left-hand margin:

--SUMMARY OF THE INVENTION--;

Page 4, line 9, delete "a" and substitute --A--;

Page 4, line 10, delete "means" and substitute --Means--;

Page 4, line 10, after "possible", insert --, while the programs are running,--;

Page 4, line 11, delete "use as working memory to" and substitute --from using--;

Page 4, line 11, after "memories", insert --to using the other working memory--;

Page 4, line 12, delete "preserving" and substitute --saving--;

Page 4, line 12, delete "content" and substitute --contents--;

Page 4, line 13, delete "these means of switching" and substitute --These switching means--;

Page 4, line 13, delete "memorizing" and substitute --storing--;

Page 4, line 14, before "context", insert --operating--;

Page 4, line 14, delete "whereby" and substitute --of--;

Page 4, line 14, delete "run through" and substitute --in--;

Page 4, line 15, delete "to validate" and substitute --enabling--;

Page 5, line 1, delete "particularity, it has" and substitute --aspect of the invention--;

Page 5, line 1, delete "memorizing the" and substitute --is provided for storing the operating--;

Page 5, line 2, delete "the run-through of";

Page 5, line 3, delete "particularity, it has" and substitute --feature of the invention--;

Page 5, line 3, delete "correlating the run-through" and substitute --de-correlating the running--;

Page 5, line 4, delete "with respect to" and substitute --from--;

Page 5, line 4, after "clock", insert --are provided--;

Page 5, line 10 and 11, delete "working memory validation circuit and the memorization register blocks" and substitute --circuit 53 for switching and enabling the working memories and the blocks of storage registers--;

Page 5, line 13, delete "replace, during use" and substitute --are substituted for the working memory and its access registers in its utilization--;

Page 5, line 13, delete ", the first memory and its own access registers";

Page 5, line 18, after "execution", insert --or running--;

Page 5, line 18, after "connection to", insert --or randomly jumping--;

Page 6, line 13, before "working" delete --smaller--;

Page 6, line 13, after "space", insert --smaller--;

Page 6, line 15, before "means", insert --switching--;

Page 6, line 15, delete "of switching substitutes" and substitute --effects substitution of--;

Page 7, line 2, delete "permit" and substitute --allow--;

Page 7, line 5, delete "means of";

Page 7, line 5, after "switching", insert --means--;

Page 7, line 6, after "back", insert --or returned--;

Page 7, line 7, delete "replacing" and substitute --substituting--;

Page 7, line 13, after "is", insert --carried out--;

Page 7, line 15, delete "from" and substitute --of--;

Page 7, before line 18", insert the following heading at the left-hand margin:

--BRIEF DESCRIPTION OF THE DRAWINGS--;

Page 7, line 18, delete "particularities" and substitute --object--;

Page 8, before line 9, insert the following heading at the left hand margin:

--DESCRIPTION OF THE PREFERRED EMBODIMENT(S)--;

Page 9, line 4, after "RAM", insert --51--;

Page 9, line 4, after "dumRAM", insert --52--;

Page 9, line 10, after "lines", insert --(533-535)--;

Page 9, line 13, delete "one of";

Page 23, after the last line 9, insert the following new paragraph:

--While this invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, the preferred embodiments of the invention as set forth herein, are intended to be illustrative, not limiting. Various changes may be made without departing from the spirit and scope of the invention as set forth herein and defined in the claims.--

IN THE CLAIMS:

Please cancel claims 1 - 19 in their entirety and substitute the following new claims:

--20. An unpredictable microprocessor or microcomputer comprising a processor (1), a first working memory (51), a main memory (6) containing an operating system a main program (P1), a secondary program (P2), a second working memory (52), switching means for switching, while the programs are running, from one of the two working memories (51, 52) to the other working memory, while saving the contents of the two working memories, access registers (A1-A3) (D1-D3) associated with each memory (6, 51, 52), said switching means comprising at least one first block of registers (54) for storing the operating context of the programs in the main memory, and a switching circuit (53) for enabling one of the working memories and the access registers (A1-A3)(D1-D3) associated with each memory (51, 52, 6) and controlled by said switching circuit (53).

21. The unpredictable microprocessor or microcomputer according to claim 20, further including a second block of registers (55) for storing the operating context of the secondary program.

22. The unpredictable microprocessor or microcomputer according to claim 20, further including means (R1, R2, R3) for de-correlating the running of the programs from an isochronous clock.

23. The microprocessor or microcomputer according to claim 20, characterized in that the main program can enable or inhibit the switching mechanism or mechanisms by loading the switching circuit (53) for switching and enabling the working memories (51, 52) and blocks of storage registers (54, 55) associated with each respective working memory (51, 52), and storing, respectively, the operating context of the programs in the main memory and the operating context of the secondary program.

24. The unpredictable microprocessor or microcomputer according to claim 20, characterized in that the second working memory (52) and its access registers (A3, D3) are substituted for the working memory (51) and its access registers (A2, D2) in utilization by a main program.

25. The unpredictable microprocessor or microcomputer according to claim 22, characterized in that the de-correlating means comprise a random number generator (2) for triggering, via an interrupt circuit (4), a random interrupt for desynchronizing the running of the programs in the processor, by randomly jumping to the secondary program (P2).

26. The microprocessor or microcomputer according to claim 23, characterized in that the de-correlating means comprise a time counting system (R3) independent from the processor (1) for, after the time count, triggering an interrupt for returning from the secondary program to the main program.

27. The unpredictable microprocessor or microcomputer according to claim 23, characterized in that the means (53, 54, 55, A2, A3, D2, D3) for switching working memories is controlled by the processor and its program, by the random interrupt system (2, 4), by a timer (R3), or by any combination of at least two of the three named elements.

28. The unpredictable microprocessor or microcomputer according to claim 20, characterized in that the means (53, 54, 55, A2, A3, D2, D3) for switching working memories is enabled

by being loaded by the processor (1) running a main program sequence.

29. The unpredictable microprocessor or microcomputer according to claim 20, characterized in that the secondary program (P2) uses a working space identical to that of the main program (P1) in the main memory (6).

30. The unpredictable microprocessor or microcomputer according to claim 20, characterized in that the secondary program (P2) uses a working space smaller than that of the main program.

31. The unpredictable microprocessor or microcomputer according to claim 20, characterized in that the switching means carry out the substitution of the memories (51, 52, 53, 54, 55, A2, A3, D2, D3) and the associated contexts within the execution cycle of an instruction from the microprocessor.

32. The unpredictable microprocessor or microcomputer according to claim 20, characterized in that the secondary program (P2) does not modify the general operating context of the main program (P1) in order to allow the main program to return without having to reestablish said context.

33. The unpredictable microprocessor or microcomputer according to claim 32, characterized in that the context of the main program (P1) is reestablished either automatically by the secondary program (P2) or automatically by the switching means (53) before returning control to the main program (P1).

34. The unpredictable microprocessor or microcomputer according to claim 20, characterized in that it further comprises means for substituting the memory of the secondary program (P2) for the memory of the main program (P1).

35. The unpredictable microprocessor or microcomputer according to claim 20, characterized in that the main program (P1) can use the first working memory (51) and/or the second working memory (52) alternately or simultaneously.

36. The unpredictable microprocessor or microcomputer according to claim 23, characterized in that loading of the switching circuit (53) makes it possible to mask or unmask de-correlating interrupts.

37. The unpredictable microprocessor or microcomputer, according to claim 25, characterized in that an interrupt

triggered by the secondary program (P2) effects return to the main program (P1) after the switching register (53) has been properly loaded, by executing an instruction of the main program (P1) or the secondary program (2), in order to unmask the interrupts.

38. The unpredictable microprocessor or microcomputer, according to claim 20, characterized in that the microprocessor or microcomputer is embodied in a monolithic integrated circuit.

39. Unpredictable microprocessor or microcomputer according to claim 21, further including means (R1,R2,R3) of de-correlating the run-through of the programs with respect to an isochronal clock.

40. Microprocessor or microcomputer according to claim 21 characterized in that the main program is adapted to enable or inhibit the switching mechanism or mechanisms by loading the switching circuit (53) of working memories (51, 52) and of the memorization register blocks (54,55) associated with each respective working memory (51, 52)

41. Unpredictable microprocessor or microcomputer according to claim 21 characterized in that the second working memory (52) and the associated access registers (A3,D3) of the second working memory are adapted to be replaced in the use thereof by a main program, with said first memory (51) and the associated access registers (A2,D2) of the first memory.

42. Unpredictable microprocessor or microcomputer according to claim 22 characterized in that the de-correlating means comprise a random generator.

43. Microprocessor or microcomputer according to claim 25 characterized in that the means of de-correlation include a time counting system (R3) independent of the processor (1) for enabling, at the end of a time count, the triggering of an interruption to return from the secondary program (P2) to the main program (P1).

44. Unpredictable microprocessor or microcomputer according to claim 25 characterized in that the means of switching (53, 54, 55, A2, A3, D2, D3) the working memories is controlled, either by one of the microprocessors and the program thereof, the random interruption system (2,4), a time

counter (R3), or a combination of at least two out of the three named elements.

45. Microprocessor or microcomputer according to claim 22 characterized in that the main program is adapted to enable or inhibit the switching mechanism or mechanisms by loading the switching circuit (53) of working memories (51,52) and of the memorization register blocks (54,55) associated with each respective working memory (51,52).

46. Unpredictable microprocessor or microcomputer according to claim 22 characterized in that the second working memory (52) and the associated access registers (A3,D3) of the second working memory are adapted to be replaced in the use thereof by a main program, with said first memory (51) and the associated access registers (A2,D2) of the first memory.

47. Unpredictable microprocessor or microcomputer according to claim 26 characterized in that the means of switching (53, 54, 55, A2, A3, D2, D3) the working memories is controlled, either by one of the microprocessors and the program thereof, the random interruption system (2,4), a time

counter (R3, or by a combination of at least two out of the three named elements.

48. Unpredictable microprocessor or microcomputer according to claim 25 characterized in that the interruption circuit (9) triggers the random generator to thereby trigger the random interrupt to desynchronize execution of the programs in the processor, by random connection to the secondary program (P2).

49. Unpredictable microprocessor or microcomputer according to claim 26 characterized in that the de-correlation includes a time counting system (R3) independent of the processor (1) for enabling, at the end of a time count, the triggering of an interruption to return from the secondary program (P2) to the main program (P1), and the means of switching (53, 54, 55, A2, A3, D2, D3) the working memories is controlled by one of the microprocessors and the program thereof, the random interruption system (2,4), a time counter (R3) or by a combination of at least two of the three named elements.

50. Unpredictable microprocessor or microcomputer according to claim 21 characterized in that the means of

switching (53, 54, 55, A2, A3, D2, D3) the working memories is confirmed by loading from the processor executing a main program sequence.--

IN THE ABSTRACT:

Please cancel the abstract at page 30 in its entirety and substitute the following new Abstract:

--Abstract

An unpredictable microprocessor or microcomputer comprises a processor (1), a first working memory (51), a main memory (6) containing an operating system, a main program (P1) and a secondary program (P2), a second working memory (52), and switching means which, during the performance of the programs, makes it possible to switch from using one of the two working memories (51, 52) to using the other working memory, while preserving their contents. Switching means comprise at least one first block of registers (54) for storing the operating context of the programs in the main memory and a switching circuit (53) for enabling one of the working memories and the access registers (A1-a3) (d1-d3) associated with each memory (51, 52, 6) and controlled by said switching circuit (53).--

Docket 6088
BULL 3630/BC

REMARKS

This Preliminary Amendment is filed to insert headings to conform the application to U.S. practice, to correct informalities in the specification, claims and abstract resulting from a literal translation of the French text, and to eliminate the use of multiple dependent claims..

Early action on the merits is earnestly solicited.

Respectfully submitted,

KERKAM, STOWELL,
KONDRACKI & CLARKE, P.C.

Edward J. Kondracki
Registration No. 20,604

Date: February 26, 1999

Two Skyline Place, Suite 600
5203 Leesburg Pike
Falls Church, VA 22041-3401
Telephone: (703) 998-3302
Telefax: (703) 998-5634

EJK:ah\amdt-pat\UGON3630-PCT-PRE

UNPREDICTABLE MICROPROCESSOR OR MICROCOMPUTER

This invention concerns an unpredictable microprocessor or microcomputer.

It is a known fact that microprocessors or microcomputers execute excessive instructions of a program recorded in memory sequentially in step with one or several timing signals referenced with respect to one of the clock signals supplied to the microprocessor or microcomputer, either internally or externally.

It has proved to be possible to become familiarized with the various phases of this method of program execution as a function of time because the execution of the instructions is in sequence, to a process predetermined by this program, generally synchronized with the clock signals that regularly time the processor. Indeed, every program generates a sequence of instructions that must be executed successively in an order known in advance, and the moments at which each instructions begins and ends are known accurately because they are executed to a predetermined process in the course of time. Therefore, in principle, it is possible to know which instruction is performed at a given moment in the processing unit of the processor because the program that is run comprises a predetermined sequence of instructions.

For instance, it is possible to determine the number of instructions executed as of the startup of the program or of the processing unit, or the time that has elapsed from an event, an external or internal reference signal or, yet again, from the reset of the processor.

This possibility of being able to observe the run-through of a program in a microprocessor or microcomputer is a major drawback when this microprocessor or microcomputer is used in high-security applications. A malevolent person could thus find out the successive states of the processor and use this information to obtain a number of sensitive results regarding internal processing.

For instance, it can be imagined that a given action may occur at different moments depending on the result of a determined security operation such as the testing of internal confidential information or the deciphering of a message or, yet again, the integrity testing of some information. Depending on the moment in question, it might be possible, for example, to act on the processor or to obtain the value of certain registers by physical investigation, and thus obtain information about the result or confidential content of the information and even, in the case of cryptographic calculations, about the secret ciphering key used.

There are devices offering an initial improvement to security microcomputers by equipping them with circuits generating random clock pulses. In this way, the observation of events makes it particularly difficult to carry out investigations because synchronization soon becomes impracticable.

However, this type of solution involves many drawbacks.

First, the design of such circuits is particularly tricky and fastidious because there is no way of simulating random operation throughout as complex a circuit as a microcomputer. It is

even more difficult to test the circuits at the end of production in terms of the scrambled behavior thereof. A random sequence of clock pulses is indeed very difficult to simulate for the definition of the circuits, but it is even more difficult to master all the behavior of all the processor logic circuits, in particular during periods of signal switching on the internal busses and in the registers.

That is why an initial improvement, the subject of the request for French Patent N° 9602903 of March 07, 1996 made by the applicant, entitled "improved integrated circuit, process for use of such integrated circuit" was made to permit the normal operation of the processor during definition and test periods with a customary periodic clock; the processor is capable of itself switching between protected mode or normal mode. To ensure security, it is easy to imagine that the mode could only be activated by the processor on entry of a password or an *ad hoc* ciphered message.

In addition to these difficulties, there is that of diagnosing failures during sequences under the control of a random clock, i.e., in a totally disordered manner. Indeed, in such disorder, how could a problem be attributed to a faulty part, and how can the exact conditions under which it appears be determined?

It can be seen that the use of a random clock, although it does offer a theoretically interesting improvement, is not a totally satisfactory solution and, above all, is not easy to implement in practice.

One of the purposes of this invention is to equip the processor with means to inhibit the type of investigation described above and, more generally, to prevent illicit observations of the internal behavior of the processor while using totally controlled standard circuits to permit a simple design and diagnosis of faults by use of conventional methods.

The purpose is achieved by the fact that unpredictable microprocessor or microcomputer, which comprises a processor, an initial working memory, a main memory containing an operating system, a main program and a secondary program, is characterized in that it also has:

- a second working memory;
- means of communication which, during the execution of the programs, make it possible to switch use as working memory to one of the two working memories while preserving their content.
- these means of switching include at least one block of registers memorizing the context whereby the programs run through the main memory and a switching circuit to validate one of the working memories and the access registers associated with each memory and controlled by said switching circuit.

According to another particularity, it has a second block of registers memorizing the context for the run-through of the secondary program.

According to another particularity, it has means of correlating the run-through of the programs with respect to an isochronal clock.

Another purpose of this invention is to ensure that the implementing of said means is assured by the processor itself, so that any additional security created by the above means depends only on a decision of the operating system located in the microcomputer and which is, therefore, unpredictable as regards malevolent action.

The purpose is achieved by the fact that the main program can enable or inhibit the switching mechanisms by loading the working memory validation circuit and the memorization register blocks associated with each working memory.

According to another particularity, the second working memory and its access registers replace, during use by a main program, the first memory and its own access registers.

A third purpose of this invention is to render the execution time independent of the program itself, but without making it necessary to use clock and random timing signals.

This goal is achieved by the fact that the decorrelation means include a random generator capable of triggering, by means of an interruption circuit, a random interrupt to desynchronize the execution of the programs in the processor by random connection to the secondary program.

According to another particularity, the means of decorrelation include a time counting system independent of processor 1 which, at the end of the time count, triggers an interrupt to return from the secondary program to the main program.

According to another particularity, the means of switching the working memories is controlled either by the processor and the program thereof or by a random interrupt system or a time counter, or by any combination of at least two out of the three.

A fourth purpose of the invention is to avoid register switching from being interpreted as a means of direct or indirect access to sensitive information.

This goal is achieved by the fact that the means of switching of the working memories is confirmed by a change from the processor carrying out a main program sequence.

According to another particularity, the second program uses a working space identical to that of the main program in the main memory.

According to another particularity, the secondary program uses a smaller working space than that of the main program.

According to another particularity, the means of switching substitutes the working memories and the associated contexts within the execution cycle of a microprocessor instruction.

According to another particularity, the secondary program does not modify the general operating context of the main program so as to permit return to the latter without any need to reestablish the context.

According to another particularity, the context of the main program is reestablished either automatically by the secondary program or automatically by the means of switching before control is transferred back to the main program.

According to another particularity, it includes means of replacing the secondary program memory for the main program memory.

According to another characteristic, the main program can use the first working memory and / or the second working memory either alternately or simultaneously.

According to another characteristic, the loading of the switching circuit enables the masking or unmasking of the decorrelation interruptions.

According to another characteristic, return to the main program is by an interrupt triggered by the secondary program after the switching register has been suitably loaded by the execution of an instruction, from the main program or secondary program, to unmask the interrupts.

According to another particularity, it consists of a monolithic integrated circuit.

Other particularities and advantages of this invention will become more evident from the reading of the description below referring to the attached illustrations in which:

Figure 1 is an electronic diagram of the integrated circuit according to one embodiment of the invention;

Figure 2 is the timing diagram of the execution of instructions on appearance of interruptions and acknowledgment of an unmasked interrupt;

Figure 3 represents an alternative design of the loading circuit of one of the integrated circuit memorization registers;

Figure 4 represents the logic diagram of the program part (P2) enabling the return to normal operation of the circuit.

Figure 1 represents one of the embodiments of the invention. The microprocessor or microcomputer covered by the invention, called the SUMIC (Self-Unpredictable MICrocomputer) comprises a monolithic integrated circuit with a processing unit (1), a non-volatile memory (6) containing the programs to be executed, a RAM (51) with its address registers (A2) and its data registers (D2), as well as a random or pseudo-random signal generator (2) which supplies, for instance, pulses at regular and unpredictable moments, an interrupt circuit (4), a register circuit (R2), a timer (R3), a sequencer circuit (8), a non-volatile memory (7) (NVM), a dummy memory (DumRAM) (52) of the volatile type with its addressing registers (A3) and data registers (D3), two register stacks (54, 55) for memorizing the parameters for return to normal operation and a switching circuit (53) comprising, for example, a register having a sufficient number of cells to check the operation of address

registers (A1) and (A3) and data registers (D1) and (D3) and a first block (54) and second block (55) of memorization registers. This switching register (53) is loaded by the processing unit (1) via the bus (3). The state of this switching register (53) is more particularly used for validating the RAM and / or DumRAM in the working memory space of the processor, or outside of this space.

In this monolithic integrated circuit, the processing unit is connected by a bus (3) to the various memories, each going toward a register having respective addresses (A1, A2, A3) and a respective data register (D1, D2, D3), each of which address and data register can be locked by a command line (531 A, 532 A, 536 A), respectively (531 D, 532 D, 536 D) leading out of switching circuit (53). This switching circuit also includes three other command lines, one of which (533) terminates at an AND gate (11) with two inputs, the second input of which receives a bus line (31) leading from the interrupt circuit. The output of this AND gate is connected directly to one of the Interrupt Enable Register (IER) bits to mask the interruption triggered by the interrupt circuit (4), but only when the switching circuit has not been activated and when, accordingly, line (533) is not active.

The two other lines (534, 535) each lock one of the two locks or stacks or memorization registers (54, 55). Each of these blocks has a number of memorization registers (54) and respectively (55) for the storage of the information which will be described below. These registers (54, 55) are connected to the bus (3) common to the memories. This bus (3) is

used for loading the switching circuit (53) with the values needed to render the control lines (531 A, 532 A, 532 D, 536 A, 536 D, 533, 534, 535) active or inactive depending on the desired operating mode. The non-volatile memory (6) contains the circuit operating system and an initial application program (P1) called subsequently the main program and a second program (P2) called subsequently the secondary program, the sequencer (8), the registers (R2), the timer (R3) and the random generator (R1) also connected to the bus (R3) and the three elements (R1, R2, R3) connected to an interrupt generator circuit (4) connected to the processor interrupt inputs (1) using on the Interrupt Enable Register (IER) of the processor, one of the bits which is generally reserved and available for applications specific to some users.

In an initial embodiment, main program (P1) contained in the non-volatile memory (6) modifies as necessary the state of switching circuit (53) through bus (3), a process that does not represent any difficulties in execution. Momentarily, this switches out the main working RAM (51) or part of this memory by acting on the CE (Chip Enable) input validating a memory package and all the registers needed for the first block (54) for return to normal operation. These memories and registers can be advantageously of the static type so as to save on the energy needed for maintaining them. The switching circuit (53), therefore, replaces the dummy memory (52) for the main working memory (51) so that the programs are executed using exclusively the dummy memory instead of the main working memory. Said dummy

memory (52) can be at the same addresses as the memory for which it is replaced but can also be at a different address. One advantageous and economical solution consists in using a very small RAM for this dummy memory. Indeed, this dummy memory does not play a functional part for the main program, and the addressable space can be restricted by simply decreasing the length of the addressing register (A3). It is also possible to "fold back" the address on itself by setting up an Exclusive OR between several address register blocks. Thus, if the addressable space of the main working memory is 512 bytes, the dummy memory can be restricted to 32 bytes without difficulty, thus leading to a very economical solution. The 32 bytes can correspond, for instance, to the simple addition of a RAM memory line to the matrix of the main working memory. In this case, this line will have its own address registers (A3) and failure registers (D3). When the switching circuit (53) activates the dummy memory, it can also inhibit any write access to the NVM so as not to disturb its content.

To carry out the switching, it is sometimes advantageous to use two blocks of registers alternately, a first block (54) and a second block (55), each containing the entire context needed for executing the program and, more particularly, the program counters respectively (PC1) for the first block (54) and (PC2) for the second block (55), the instruction decoding registers (D1) for the first and (D2) for the second, and other registers symbolized by (T11, T12 and T21, T22). The latter registers (T11, T12, T21 and T22) preserve the same operating parameters such as, for example, the machine cycle number to be used. All these registers are

switched automatically by switching circuit (53). The change of address is carried out instantly in this case without there being any obligation, as in the case of most micro-calculators, to save the content of the program counter in a register stack using a specific instruction. Thus, switching in both directions is very fast (generally much shorter than a clock cycle), considerably increasing the security level of the device. The same mechanism can be used for the other registers which save the operating context of the processor, like (T11 to T22).

It should be understood that when program (P1) activates the operation of the integrated circuit in the dummy mode by loading the switching register, the switching circuit (53) will inhibit the first stack of registers (54) which preserves the parameters prior to the dummy circuit operation to restart it where the program (P1) has been interrupted. On the other hand, the second stack of registers (55) will be used to enable normal operation of the circuit with the same dummy memory to execute program (P2). It is also evident that, in this case, the interrupt masking IER register bit corresponding to operation in the dummy mode will have been unmasked so as to enable, during the generation of an interrupt either by the random generator or by the timer (R3) previously loaded by the random generator with a random number, and at the end of the run-through of the time represented by this number, or by register (R2) loaded with specific information, triggering the interruption, (31) causing changeover from normal operation under control of program (P1) to operation in the dummy mode under the control of program (P2).

Figure 2 illustrates operation in the interrupt mode. The diagram shows that the first interrupt pulse IT, transmitted by the interrupt circuit on line (31) toward the processing unit (1), is not taken into consideration because it was masked by means of the register and the interrupt masking using the instruction "MOVE immediate data to register IER" so as to load the data into the masking register. It is assumed that the current instruction unmasks the diversion interruption (but this can be done by any other instruction at a different time). In this case, the second pulse is considered by the processing unit (1) causing the switching circuit (53) to switch over and, accordingly, the second block of registers (55) and the DumRAM (52) become active instead of the first block (54) and the RAM dummy memory (51). It is to be noted that the acknowledging of the interruption is only possible during the transition from one state to another, for instance between (S2) and (S3) so as to memorize a stable and consistent state of the machine and, above all, to restore exactly the same state when the interrupted program returns. If this interruption is acknowledged, as is the habitual case at the end of an instruction, there is no particular problem when the interrupted program is recovered because it takes place normally on the next instruction. Conversely, if the interruption occurs during the execution of an instruction, for example in state (S2), it is obviously necessary for the sequencing circuits to be reestablished identically so as to correctly trigger the state (S3) on recovery of the interrupted program. This can be achieved, for instance, by a direct link between the register (T11) and the sequencer (8) via the bus (3) at the moment of recovery.

This link can also be specific without going via the bus (S3). It might also be advantageous to include the status memorization registers in the sequencer itself to avoid the mobilization of the bus during this phase.

In this way, by means of an interruption, the main program (P1) can enable and / or switching to a secondary program (P2) as described below. When the secondary program is no longer active, the state of switching circuit (53) changes and the RAM working memory regains its initial configuration without any modification so that the main program can recover its course exactly at the point it was interrupted. It can also be carried out in such a way that when the main program (P1) needs to be protected, by its own diversion of a secondary program (P2), it trips and generates a random length at moments chosen by it, either at the beginning or during the processing, so as to scramble the different sequences. The operation of the process can then be controlled by the secondary program (P2) which, for example, can trigger a waiting loop of which the length of time depends on a random number derived from the generator (2). The secondary program can be executed using the parts of the memory unused by the main program so that the latter can resume its normal process as soon as the secondary program transmits the new control to it, or yet again, on the next interruption, or once again, using the timer as previously, or using a combination of the two. The secondary program can also use the shared resources as long as it reestablishes the context of the main program before transferring control back to it.

It might be tempting to say that these mechanisms are similar to the execution of the branching of the main program towards a secondary program with return at the end of the execution of the latter but that of the invention is particularly different:

- the secondary program does not execute any function mandatorily related to the main program,
- the size of the dummy memory (52) can be much smaller than needed for the normal run-through of a program
- the content of the dummy memory (52) is of no importance because it simply covers the tracks
- with this fast mechanism, it is possible to interlace the instructions of the secondary program with those of the main program
- there is no need to save the context of the secondary program because the latter is used simply for covering tracks.

In a second embodiment, when the processor switches the circuit (53) at the same time, it activates a timer (R3) initialized either by random generator (2) or from the content of non-volatile memory NVM (7). Said NVM of the E2 PROM type, for instance, or a ferro-electric unit, can indeed contain a single number modified each time the NVM is used. When the

timer (R3) expires, after an unpredictable period of time, it triggers return to the main program and also switches the switching circuit (53) to bring the main memory back into the working space. This mechanism can be executed either by a conventional interruption or by direct action of the timer (R3) on the switching circuit (53) and by action on registers (PC1) and (PC2), checking the execution of the programs by the processing unit (1) such as (PC1) and (PC2).

'In an alternative embodiment, it is possible to use as secondary program (P2), any part of main program (P1) initially pointing to an address chosen at random then inverting the bytes obtained from the address and / or inverting, for example, the content of register (ID2) by reverse cabling or by a left shift circuit for the content of an address. In this way, we can also be assured that the program will execute totally outlandish instructions.

Another alternative for the execution of outlandish instructions can be that provided in Figure 3 wherein a register decoding temporary instructions IDT is connected, on the one hand, to the bus (3) by a portion of bus (33) and, on the other hand, to the second stack of registers (55) enabling the memorizing of the circuit states by a portion of the bus (34). The portion of bus (34) is connected by hardware to register (ID2) of stack (55) by specific cabling connecting bit (B7) of register IDT to bit (B4) of register (ID2), bit (B6) of register IDT to bit (B1) of register (ID2), bit (B5) of register IDT to bit (B3) of register (ID2), etc.

Finally, a final alternative allows the execution (of instructions) that are totally outlandish and comprises and embodiment as depicted in Figure 3 in which the bus (3) is connected by a portion of bus (35) to the IDT temporary instructions decoding register. Another portion (37) of the bus connects this IDT register to an exclusive OR gate (39) with several inputs. The other inputs of this OR gate are connected by a bus (38) to a register (R'2) loaded with a portion (36) of the bus bringing it into relation with bus (3). This register (R'2) can be loaded with any information such as that obtained from a random generator (R1) or a timer or a non-volatile memory NVM (7) by an instruction such as "MOVE register (R1) (for instance) to register (R'2)". This type of shift instruction is well known to the man of the art in the field of microprocessors and does not involve any difficulties of implementation. The exclusive OR between the information from register (R'2) and the values loaded into the IDT register are a way of totally modifying the program instructions (P2) and, thus, executing totally outlandish instructions.

It is possible to use in the program (P2), a multitude of sequences which will be called in a random manner and each of the sequences will implement a set of different instructions entailing a variable processing time in each branch and different microprocessor behaviors. The sequences can be called at random, for instance after the main program has carried out the jump to the secondary program, the latter of which loads a random value V from memory (7) into two registers, for example (T21) and (T22) of microprocessor (1). The secondary

program increments this value V then the program commands the memorizing of this value, incremented in non-volatile memory (7). This value, memorized in the non-volatile memory (7) is designed for subsequent use. The secondary program then samples n MSBs or LSBs in (T21) to obtain a value r making it possible to designate the program sequence to be executed from the various secondary program sequences.

In a third embodiment, the random generator (2) can be interrogated by the processor (1) via the bus (3) by a read instruction in order to find out its status, or by directly reading a determined pulse or by grouping several of them or yet again by considering the content of register (R2) loaded from random generator 92). When the main program needs protection, it transfers control to the secondary program in a similar way to the mechanism seen previously.

Naturally, it is possible to combine the effects of the previous embodiments by having, on the one hand, a random clock and, on the other, the possibility of interrupting the run-through of the main program either by itself or by a random interruption system which it either authorizes or not.

It is also evident that the run-through of the main program is accomplished according to absolutely unpredictable sequencing which depends either on the random generator or on the program or on the timer or on the secondary program or on two, three or four elements at a time. When the main program executes functions that are not sensitive from the security point of view, it can also have recourse to normal operation for instance, to supply results to the

outside world or to mask the timer (R3) or random generator (2) decorrelation interruptions and, thus, optimize the processing time. As soon as a security function is implemented, the principal program (P1) enables operation in the random mode by validating the decorrelation interruptions so as to "scramble" the operation.

A fourth embodiment also illustrated in Figure 1 allows the use of RAMs (51) and (52) simultaneously. Indeed, if it is assumed that it is possible to detect the switching of the memories and the associated registers, it might be possible to carry out analyses by eliminating the sequences using the dummy memory (52). To avoid this eventuality, this embodiment means that the memories (51) and (52) can be validated in parallel during an initial phase. Obviously, this presupposes that memory (52) in the case at hand, has a size equal to at least that of the zone used by program (P1) in memory (51) when working with the latter. In this way, the content of the two memory zones used by program (P1) respectively in memories (51) and (52) are initialized and used by this program in an identical manner during this first phase. One alternative may consist in validating by loading switching circuit (53) with the necessary configuration only one of the two registers (D2) or (D3) during the read cycles to prevent any conflicts but this does not make any fundamental change to the invention. Therefore, we cannot distinguish which memory is really used during this phase. Accordingly, during a second phase, it becomes possible to switch the memories alternately and randomly by means of modifications to switching circuit (53) while continuing to execute the same program (P1).

Therefore, it will no longer be possible to correlate the execution of one program or another with the RAM or with the registers used. In a third phase, we will switch to the dummy memory (52) via program (P2) as described previously at unpredictable moments while return to the main working memory (51) will also take place at unpredictable moments and the process will be reproducible at will under the control of the main program (T1) as a protective measure.

Finally, the last program raised by the invention is that of being able to exit from the dummy mode of the program (P2) and return to the normal operating mode with program (P1). Just before transferring control to program (P2), program (P1) will enable interruptions coming either from the random generator or from the timer while initializing the latter. During the run-through of anarchical program (P2), an interruption via the circuit (4) occurs which transfers to the interruption program (PIT). This program, accessed conventionally by means of an interruption vector, analyzes the execution context of the current program, for example. If (P2) is active, PIT transfers control to program (P1). This mechanism can be performed as follows: when the first instructions of the PIT program are executed, it can be made up, for instance, as shown in Figure 4, by the reading (41) of the content of the switching circuit (53), then a test (42) to determine whether the information contained in circuit (53) corresponds to dummy mode operation. In the affirmative, the PIT program executes a program return instruction (P1) represented by Step (43). This return is initiated by

the writing of switching register (53) according to Step (44) which consists in modifying the values of the lines (534) and (531). This subsequent writing (44) into the switching register (53) makes it possible to return to the normal modified mode of line values (534) and of line (531) so as to authorize the use of the stack (54) and of main working memory (51) once again. This instruction for return to program (P1) can be executed directly after dummy test (42) or after the execution of a number of other instructions that are not represented and which make it possible to generate a random time. If test (42) is negative, the program continues to Step (45) by writing into the switching register (53) to change over to the dummy mode so as to modify the values of lines (535) and (532) to enable the use of register stack (55) and of the dummy memory while locking the circuits under control by (531) and (534).

It will be noted that, in all said embodiments, there is no need to use a random clock. To the contrary, clock distribution can remain totally conventional and isochronal to provide easy design of the circuits and the simulation and testing thereof. In reality, security is no longer due to the fact that the processor is timed at random but rather due to the execution as such of these programs in step or not in step with an isochronal clock; execution itself is scrambled.

The organization of the programs executed by the processor can be accomplished in such a way that the operation of the processor is controlled by a real security operation system deciding on the type of jamming to be implemented according to the type of program executed

by the machine. In this case, the operating system manages, as it deems fit, the various signals coming in from the random generator, the interruptions and the launching of the main and secondary programs. Obviously, the secondary program can be used to carry out other functions than a simple waiting loop, in particular processing that can be effective for the main program so as to take advantage of the time devoted to the secondary program. This processing can comprise, for example, preparatory calculations used subsequently by the main program. Naturally, it is easy to generalize the mechanisms of the invention when the processor operates in a multi-application mode while the application programs can then be considered as simple main programs.

The random generator and timer mentioned above do not cause any particular problems in production and are known to the man of the art when used separately for other uses having no tie with this invention.

For the random generator, it is possible, for instance, to use looped counters having different periods. These counters are initialized by initialization information stored in the non-volatile memory (7). When the processor starts, the counters take the value stored as initial value into consideration. During calculation or at the end, z, the non-volatile memory is updated with a new value used as initialization information to initialize the counters on the next initialization. The generation of the interruption pulses mentioned above can then occur when the generated number has characteristics such as equality with some of the program data. It is

also possible to use the value of one or several bits of one or several counters. It is also possible to produce a very good random generator using a cryptographic algorithm or a chopping function initialized by the initialization information mentioned above. In this case, the generator can be a program implementing the algorithm. It is evident that this random number generator can also be used to generate a variety of random numbers as mentioned above. Another way of producing a generator like this is to amplify the voltage generated across the terminals of the "noise diode" and to shape the signals after low-pass filtering to ensure that excessively fast noise pulses do not interfere with the operation of the microprocessor.

CLAIMS

1. An unpredictable microprocessor or microcomputer comprising a processor (1), a first working memory (51), a main memory (6) containing an operating system a main program (P1) and a secondary program (P2), characterized in that it also has:

- a second working memory (52);

- switching means that make it possible, while the programs are running, to switch from using one of its two working memories (51, 52) to using the other working memory, while saving their contents;

- these switching means comprising at least one block of registers (54) for storing the operating context of the programs in the main memory, and a switching circuit (53) for enabling one of the working memories and the access registers (A1-A3)(D1-D3) associated with each memory (51, 52, 6) and controlled by said switching circuit (53).

2. The unpredictable microprocessor or microcomputer according to claim 1, characterized in that it has a second block of registers (55) for storing the operating context of the secondary program.

3. The unpredictable microprocessor or microcomputer according to any of the preceding claims, characterized in that it has means (R1, R2, R3) for de-correlating the running of the programs from an isochronous clock.

4. The microprocessor or microcomputer according to any of the preceding claims, characterized in that the main programs can enable or inhibit the switching mechanism or mechanisms by loading the circuit (53) for switching and enabling the working memories (51, 52) and the blocks of storage registers (54, 55) associated with each respective working memory (51, 52).

5. The unpredictable microprocessor or microcomputer according to any of the preceding claims, characterized in that the second working memory (52) and its access registers (A3, D3) are substituted for the working memory (51) and its access registers (A2, D2) in its utilization by a main program.

6. The unpredictable microprocessor or microcomputer according to claim 3, characterized in that the de-correlating means comprise a random number generator (2) that makes it possible to trigger, via the interrupt circuit (4) a random interrupt for desynchronizing

the running of the programs in the processor, by randomly jumping to the secondary program (P2).

7. The microprocessor or microcomputer according to claim 4 or 6, characterized in that the de-correlating means comprise a time counting system (R3) independent from the processor (1) that makes it possible, after the time count, to trigger an interrupt for returning from the secondary program to the main program.

8. The unpredictable microprocessor or microcomputer according to claim 4, 6 or 7 or a combination thereof, characterized in that the means (53, 54, 55, A2, A3, D2, D3) for switching working memories is controlled by the processor and its program, by the random interrupt system (2, 4), by a timer (R3), or by any combination of at least two of the three.

9. The unpredictable microprocessor or microcomputer according to any of the preceding claims or a combination thereof, characterized in that the means (53, 54, 55, A2, A3, D2, D3) for switching working memories is enabled by being loaded by the processor (1) running a main program sequence.

10. The unpredictable microprocessor or microcomputer according to any of the preceding claims, characterized in that the secondary program (P2) uses a working space identical to that of the main program (P1) in the main memory (6).

11. The unpredictable microprocessor or microcomputer according to any of claims 1 through 9, characterized in that the secondary program (P2) uses a working space smaller than that of the main program.

12. The unpredictable microprocessor or microcomputer according to any of the preceding claims, characterized in that the switching means carry out the substitution of the memories (51, 52, 53, 54, 55, A2, A3, D2, D3) and the associated contexts within the execution cycle of an instruction from the microprocessor.

13. The unpredictable microprocessor or microcomputer according to any of the preceding claims, characterized in that the secondary program (P2) does not modify the general operating context of the main program (P1) in order to allow the latter to return without having to reestablish this context.

14. The unpredictable microprocessor or microcomputer according to claim 13, characterized in that the context of the main program (P1) is reestablished either automatically by the secondary program (P2) or automatically by the switching means (53) before returning control to the main program (P1).

15. The unpredictable microprocessor or microcomputer according to any of the preceding claims, characterized in that it comprises means for substituting the memory of the secondary program (P2) for the memory of the main program (P1).

16. The unpredictable microprocessor or microcomputer according to any of the preceding claims, characterized in that the main program (P1) can use the first working mer (51) and/or the second working memory (52) alternately or simultaneously.

17. The unpredictable microprocessor or microcomputer characterized in that the loading of the switching circuit (53) makes it possible to mask or unmask the de-correlatin interrupts.

18. The unpredictable microprocessor or microcomputer, characterized in that th return to the main program (P1) is carried out by an interrupt triggered by the secondary

program (P2) after the switching register (53) has been properly loaded, by executing an instruction of the main program (P1) or the secondary program (2), in order to unmask the interrupts.

1. 19. The unpredictable microprocessor or microcomputer, characterized in that it is embodied in a monolithic integrated circuit.

ABSTRACT

This invention concerns an unpredictable microprocessor or microcomputer including a processor (1), a first working memory (51), a main memory (6) containing an operating system, a main program (P1) and a secondary program (P2) characterized in that it also includes:

- a second working memory (52);
- switching means which, during the performance of the programs, makes it possible to switch use as working memory towards either of the two working memories (51, 52) while preserving the content thereof;
- these switching means include at least one block of registers (54) to memorize the context for the run-through of the programs in the main memory and a switching circuit (53) for the validation of the working memories and the access registers (A1-A3) (D1-D3) associated with each memory (51, 52, 6) and controlled by said switching circuit (53).

Figure 1

Docket 6088
BULL 3630/BC

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)

Applicant:	Michel UGON
International Application No.:	PCT/FR98/01343
International Filing Date:	25 June 1998
U.S. Serial No.:	To be Assigned
U.S. Filing Date:	February 26, 1999
For:	"UNPREDICTABLE MICROPROCESSOR OR MICROCOMPUTER"

Falls Church, Virginia

PROPOSED DRAWING CORRECTIONS

Hon. Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

Applicant requests approval of the drawing corrections in Figs. 1 - 3 as shown in red on the attached three (3) sheets.

The proposed corrections only comprise labeling of blocks with the French terms translated into English and

removing the headings "1/3" to "3/3" to conform the drawings to U.S. practice.

Respectfully submitted,

KERKAM, STOWELL,
KONDRACKI & CLARKE, P.C.

Edward J. Kondracki
Registration No. 20,604

Date: February 26, 1999

Two Skyline Place, Suite 600
5203 Leesburg Pike
Falls Church, VA 22041-3401
Telephone: (703) 998-3302
Telefax: (703) 998-5634

EJK:ah\amdt-pat\UGON-3630-PCT-DRA

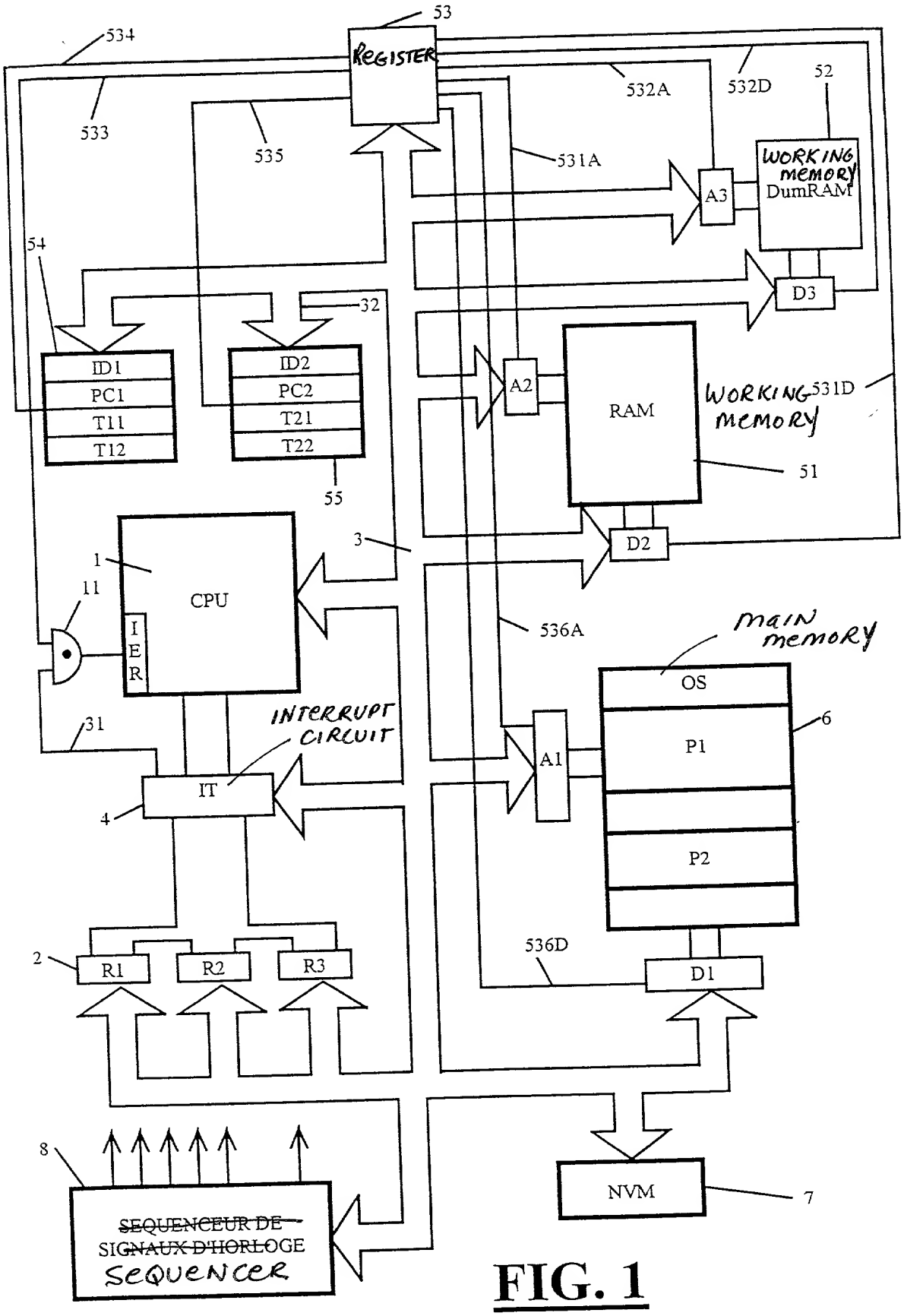
53
534
REGISTER
532A
532D
52
533
535
531A
WORKING MEMORY
DumRAM
A3
54
D3
32
ID1
PC1
T11
T12
ID2
PC2
T21
T22
A2
RAM
WORKING MEMORY
531D
51
55
3
D2
1
11
CPU
I
E
R
536A
main memory
OS
P1
P2
6
31
INTERRUPT CIRCUIT
A1
IT
4
2
R1
R2
R3
536D
D1
8
NVM
7
SEQUENCEUR DE SIGNAUX D'HORLOGE
SEQUENCER

FIG. 1

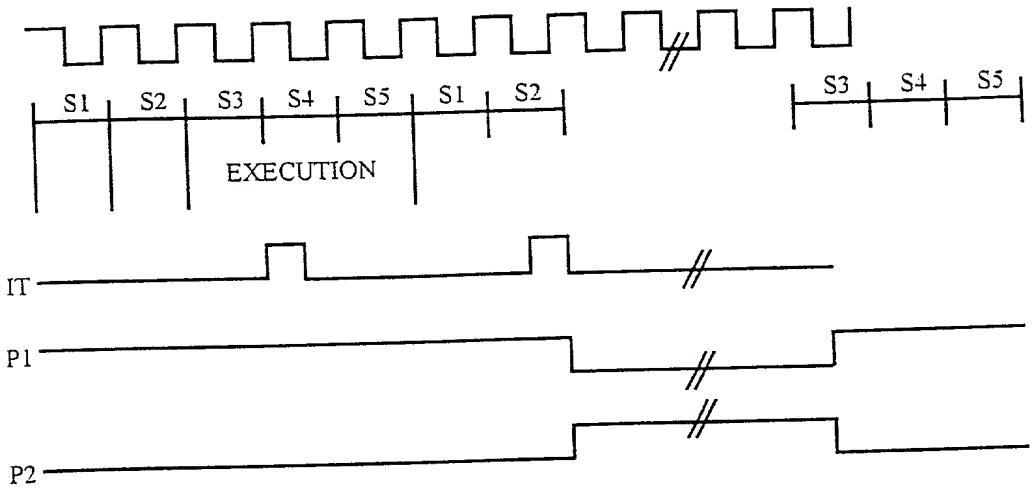
S1
S2
S3
S4
S5
S1
S2
S3
S4
S5
EXECUTION
IT
P1
P2

FIG. 2

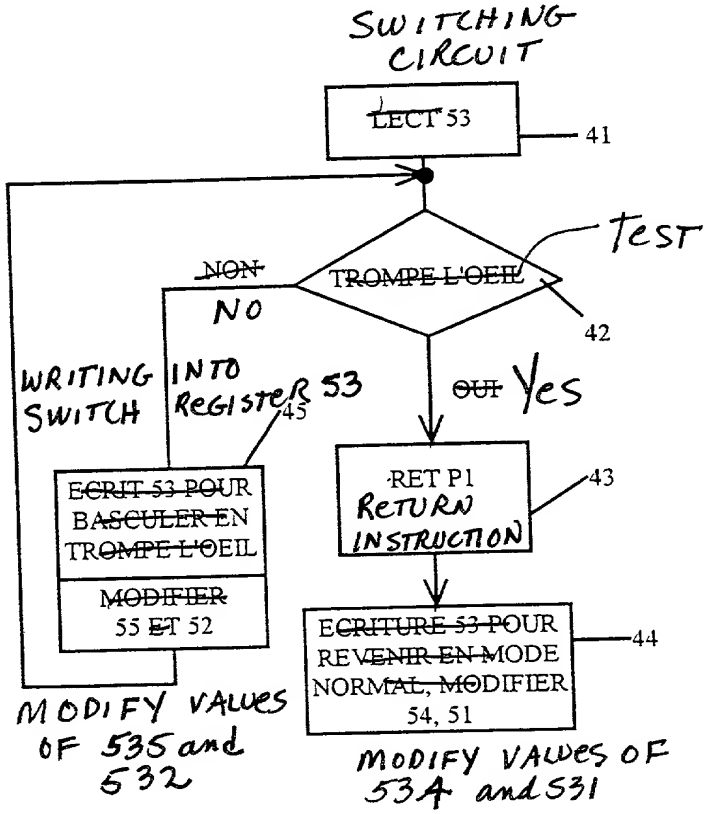
SWITCHING CIRCUIT
LECT 53
41
TROMPE L'OEIL
Test
NON
NO
42
WRITING SWITCH
INTO REGISTER 53
OUI
Yes
45
ECRIT 53 POUR BASCULER EN TROMPE L'OEIL
MODIFIER 55 ET 52
RET P1
RETURN INSTRUCTION
43
ECRITURE 53 POUR REVENIR EN MODE NORMAL, MODIFIER 54, 51
44
MODIFY VALUES OF 535 and 532
MODIFY VALUES OF 534 and 531

FIG. 4

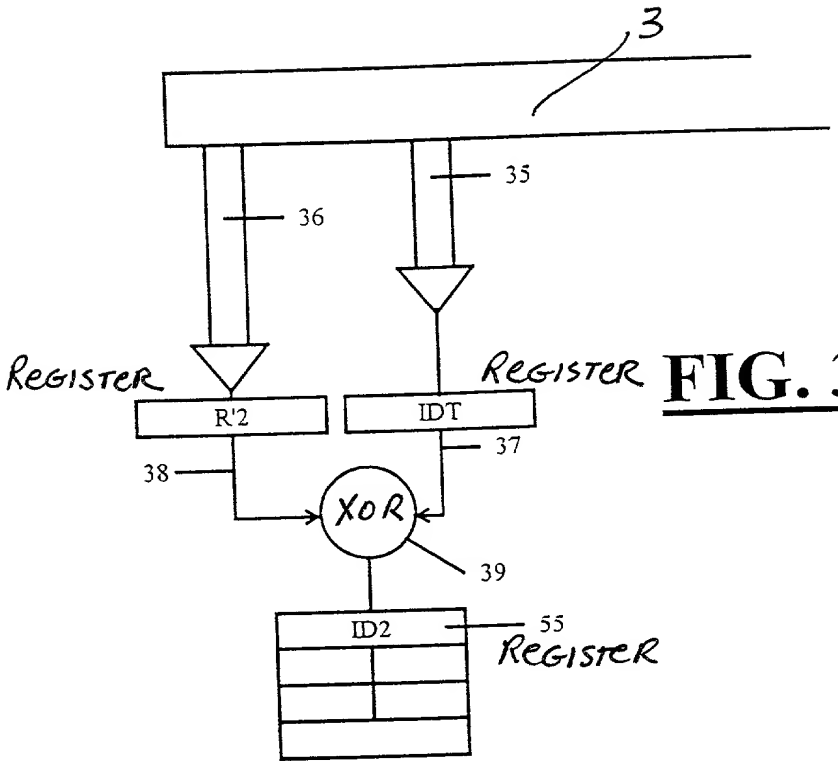
3
35
36
REGISTER
REGISTER
R'2
IDT
37
38
XOR
39
ID2
55
REGISTER

FIG. 3B

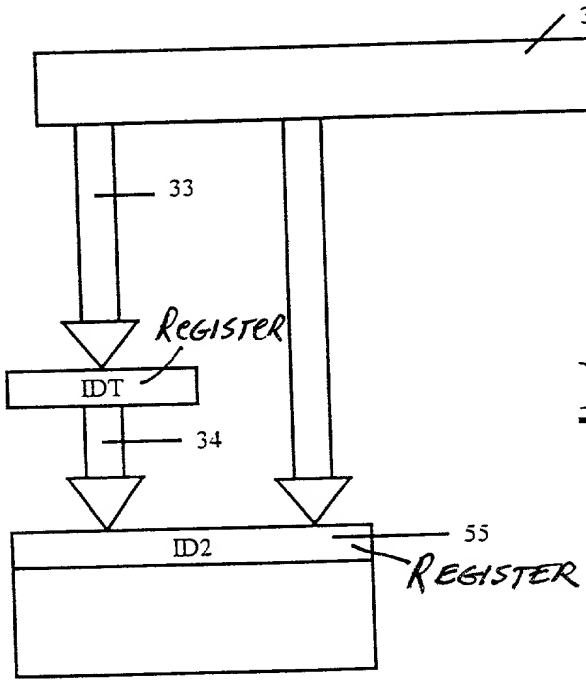
3
33
REGISTER
IDT
34
ID2
55
REGISTER

FIG. 3A

Declaration and Power of Attorney For Patent Application
Declaration Pour Demandes de Brevets Avec Pouvoirs
French Language Declaration

En tant qu' inventeur nomme ci-après, Je déclare par le présent acte que:

As a below named inventor, I hereby declare that:

Mon nom, mon domicile, mon adresse postale, ma nationalité sont ceux qui figurent ci-après,

My residence, post office address and citizenship are as stated below next to my name,

Je déclare que je crois être l'inventeur original, premier et unique (si un seul nom figure sur le présent acte) ou un des co-inventeurs, originaux et premiers (si plusieurs noms figurent sur le present acte) du sujet revendiqué et pour liquel un brevet est demande sur la base de l'invention intitulée:

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

Microprocesseur ou microcalculateur imprévisible.

dont la description
(cocher la case correspondante)

the specification of which
(check one)

☒ est annexée au présent acte.

☐ a été déposée _____

Numéro de série de la demande _____

et modifiée le _____ (si approprié)

☐ is attached hereto.

☐ was filed on _____ as

Application Serial No. _____

and was amended on _____ (if applicable)

Je déclare par le présent acte avoir examiné et compris le contenu de la description identifiée ci-dessus, revendications y compris, et le cas échéant telle que modifiée par l'amendment cité plus haut.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

Je reconnais le devoir de divulguer l'information qui est en rapport avec l'examen de cette demande selon Titre 37 du Code des Reglements Fédéraux §1.56(a).

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

French Language Declaration

Je revendique par le présent acte le bénéfice de priorité étrangère selon Titre 35, du Code des Etats-Unis, §119 de toute demande de brevet ou d'attestation d'inventeur énumérée ci-après, et j'ai identifié également ci-après toute demande étrangère de brevet ou d'attestation d'inventeur ayant une date de dépôt antérieure à celle de la demande pour laquelle la priorité est revendiquée.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior foreign applications

Demande(s) de brevet antérieure(s) dans un autre pays:

(Number) (Numéro)	(Country) (Pays)	(Day/Month/Year Filed) (Jour/Mois/Année de dépôt)	Priority claimed / Droit de priorité revendiqué: Yes Oui	No Non
FR 97 07995	FRANCE	26.06.97	☒	☐
			☐	☐
			☐	☐

Je revendique par le présent acte, le bénéfice selon Titre 35 du Code des Etats-Unis, §120 de toute(s) demande(s) américaines énumérée(s) ci-après et, dans la mesure où le sujet de chacune des revendications de cette demande n'est pas divulgué dans la demande américaine antérieure, de la façon dèfinie par le premier paragraphe de Titre 35 du Code des Etats-Unis, §112, je reconnais le devoir de divulguer l'information pertinente selon Titre 37 du Code des Réglements Fédéraux, §1.56(a), toute information qui se présente entre la date de dépôt de la demande antérieure et la date de dépôt de la demande, soit nationale, soit internationale PCT.

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.) (No. de Demande)	(Filing Date) (Date de Dépôt)	(Etat) (brevetée, pendante, abandonné)	(Status) (patented, pending, abandoned)
PCT/FR 98/01343	25.06.98	PCT	pending

Je déclare par le présent acte que toutes mes déclarations, à ma connaissance, sont vraies et que toutes les déclarations faites à partir de renseignements ou de suppositions, sont tenues pour être vraies; de plus, toutes ces declarations ont été faites en sachant que de fausses déclarations volontaires u autres actes de même nature sont sanctionées par une amende ou un emprisonnement, ou les deux, selon la Section 1001, du Titre 18 de Code des Etats-Unis et que de selles déclarations délibérément fausses peuvent compromettre la validité de la demande ou du brevet délivré.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

French Language Declaration

POUVOIR: En tant qu'inventeur, je désigne l'(les) avocat(s) et/ou l'(les) agent(s) suivant(s) pour poursuivre la procédure de cette demande et traiter toute affaire la concernant supris du Bureau des Brevets et de Marques:

Harold L. Stowell, Reg. 17,233
Edward J. Kondracki, Reg. 20,604
Dennis P. Clarke, Reg. 22,549
William L. Feeney, Reg. 29,918
John C. Kerins, Reg. 32,421

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (*list name and registration number*)

Harold L. Stowell, Reg. 17,233
Edward J. Kondracki, Reg. 20,604
Dennis P. Clarke, Reg. 22,549
William L. Feeney, Reg. 29,918
John C. Kerins, Reg. 32,421

Adresser toure correspondance à:

Edward J. Kondracki, Esq.
KERKAM, STOWELL, KONDRACKI
& CLARKE, P.C.
5203 Leesburg Pike, Suite 600
Falls Church, VA 22041

Send Correspondence to:

Edward J. Kondracki, Esq.
KERKAM, STOWELL, KONDRACKI
& CLARKE, P.C.
5203 Leesburg Pike, Suite 600
Falls Church, VA 22041

Adresser toute communication téléphonique à: (*Nom*) (*Numéro de téléphone*)

Edward J. Kondracki, Esq.
(703) 998-3302

Direct Telephone Calls to: (*name and telephone number*)

Edward J. Kondracki, Esq.
(703) 998-3302

Nom complet du seul ou premier inventeur	Full name of sole or first inventor
UGON Michel	
Signature de l'inventeur Date 11/26/92	Inventor's signature Date
Domicile 06 rue des Cépages, 78310 MAUREPAS, France FRX	Residence
Nationalité Française	Citizenship
Adresse Postale 06 rue des Cépages, 78310 MAUREPAS, France	Post Office Address
Nom complet du second co-inventeur, le cas echeant	Full name of second joint inventor, if any
Signature de l'inventeur Date	Second Inventor's signature Date
Domicile	Residence
Nationalité	Citizenship
Adresse Postale	Post Office Address

(Fournir les mêmes renseignements et la signature de tout co-inventeur supplémentaire.)

(Supply similar information and signature for third and subsequent joint inventors.)